

REMARKS

As a preliminary matter, Applicants acknowledge and appreciate the Examiner's withdrawal of the objection to the drawings and specification, as well as the Examiner's withdrawal of the claim rejections under 35 U.S.C. § 112, second paragraph. Applicants further acknowledge and appreciate the Examiner's statement that claims 2-7, 9-23, and 25-29 would be allowable if rewritten in independent form. Applicants have amended claim 24 to incorporate allowable dependent claim 25, and to correct an informality by changing "fourth transmitting" to "second transmitting." At this time, Applicants elect to keep the remaining objected-to claims in their present form, pending the Examiner's response to the remarks submitted herein. Applicants also have amended claims 18, 26, 38, and 50 to remove informalities found by Applicants. Because the amendments do not introduce new matter, and do not require additional search or consideration by the Examiner, entry of these amendments is respectfully requested.

Claims 38-45 and 51-55 stand rejected under 35 U.S.C. § 102(e) as being anticipated by Mengin. To correct an informality found by Applicants, claim 38 has been amended to more clearly define at least that the ticket buyer's computer comprises means for combining the digital signature of the non-invertible transformation with the number to produce a digital ticket. No new matter is presented, as this feature is clearly provided in the specification (and in other claims), and was already present in claim 38, in the feature "wherein the received digital signature of the non-invertible transformation is combined with the number to produce a digital ticket." Because the feature is already defined in the claim,

Applicants respectfully submit that no new issues are presented requiring additional search or consideration, and thus request entry of the amendment. As applied to the claims as amended, Applicants respectfully traverse the rejection for at least the following reasons.

In response to Applicants' previous remarks, the Office Action indicates that the Examiner would reconsider the rejection if Applicants clearly state "what exactly" the claimed process solves over the prior art "since the summary of the invention [does not] define such a process." However, Applicants wish to point out that several portions of the specification (e.g., page 36, line 25 – page 42, line 8) explicitly and clearly explain benefits that embodiments of the invention solve over prior art processes.

Generally, preferred embodiments of the present invention provide a way to produce a digital ticket between two parties (e.g., a buyer and a seller) that: significantly limits the ability of either of the two parties (the buyer or the seller) to commit fraud; optionally allows one of the parties (the buyer) to anonymously purchase the ticket; and does not require a third party (e.g., a certification authority as in Rosen) to certify both the first and the second party. Benefits of mutual security are provided according to preferred embodiments by specifying which party provides what part of the ticket, and in what order.

Contrary to the Office Action's statement, "Switching a process from one location to another is not Novel nor an inventive step over Prior Art of records," the location of each step in the process, and the order in which the steps are performed, provide one or more of these benefits, and are neither taught nor suggested by the cited references. Applicants acknowledge that hashing, digital signatures, and digital certification are known

in the art, as are random numbers. However, the invention as claimed is more specific, and more clearly defined, than the general computer terms listed in the Office Action.

For example, page 36, line 25 – page 42, line 8 specifically and clearly states that, according to embodiments of the claimed system, the ticket consumer's computer produces something that the ticket provider's computer cannot produce before ticket redemption. This provides security for the ticket buyer. In amended claim 38, this is due at least to the data representative of a non-invertible transformation of a number determined by the ticket buyer only, and due to the ticket buyer (not the seller) combining the digital signature of the non-invertible transformation with the number to produce the ticket.

However, in Mengin, the “digimas” is composed by one party (the seller) only, and is also hashed and encoded only by that party. The encoded, hashed number then is submitted to the ticket buyer for printing (see paragraphs 75-78 of Mengin and FIG. 2B). Though another party (the buyer) can supply information to the seller that eventually is used for composing the message before the “digimas” is created, only one party (the seller) produces a number (“digimas”), hashes the number, encodes the hashed number, and produces the ticket (e.g., sends the digital ticket contents to be printed to the buyer). Thus, unlike the system defined in amended claim 38, Mengin fails to provide protection for two parties (the buyer and the seller) by generation of the ticket, but instead only one party (the seller) is trusted.

Accordingly, Applicants respectfully request reconsideration and withdrawal of the rejection as to amended claim 38 and dependent claims 39-44. Further, as to rejected

dependent claim 39, Applicants respectfully submit that the random number defined is important in the operation of preferred embodiments, at least because it provides additional protection for the buyer by preventing the ticket seller from determining the number until redemption of the ticket. Mengin teaches away from the use of a random number as generated by the ticket buyer, or generally by a party other than the party that generates the digital signature.

Regarding claim 45, mutual security is provided at least by defining a ticket containing a one-way function of a number provided by one party (the holder of the ticket) that is digitally signed by another party (the provider). By contrast, in Mengin, as stated above, a number, a one-way function of the number, and the digital signature of the one-way function of the number are all generated by the same party (the provider), and thus the process taught in Mengin fails to provide the benefits described above. Though a holder of a ticket can provide data that may be concatenated by the provider to help generate the number, the number itself is provided only by the holder of the ticket. This is for the protection of the ticket provider in Mengin.

Thus, Mengin clearly fails to teach at least this claimed feature, and the rejection (an anticipation rejection) as to claim 45 should be withdrawn. Further, Applicants respectfully submit that it would not have been obvious, absent impermissible hindsight, to select the entities to perform the multiple steps in the claimed process. Knowledge that a process potentially can be copied or processed by any entity does not itself render the claimed steps or features obvious.

As to independent claim 51, the mutual benefit of protection for a buyer and a seller is provided at least by the features of: sending from a computer of a ticket buyer to a computer of a ticket seller a secure transformation of a number determined by the ticket buyer only and unknown to others including the ticket seller; sending from the computer of the ticket seller to the computer of the ticket buyer a secure second transformation of the secure first transformation; and storing with the computer of the ticket buyer the number in accompaniment to the secure second transformation. Particularly, by the ticket buyer providing a secure transformation of a number determined by the ticket buyer only and unknown to others including the ticket seller, and by storing with the computer of the ticket buyer the number in accompaniment to the secure second transformation, the ticket provider gains protection from possible fraud on the part of the ticket seller. Further, by sending from the computer of the ticket seller to the computer of the ticket buyer a secure second transformation of the secure first transformation, the ticket seller gains protection from possible fraud on the part of the ticket buyer. Additionally, by storing with the computer of the ticket buyer the number in accompaniment to the secure second transformation, the ticket seller and ticket buyer also gain the ability to confirm the validity of the ticket without necessarily resorting to third party verification.

In Mengin, by contrast, the number is not determined by the ticket buyer only, but is determined by the ticket seller. Further, any secure transformation as defined is performed by the ticket seller, not the ticket buyer. Still further, any second secure transformation as defined is also performed by the ticket seller. Mengin also fails to teach or

suggest storing with the computer of the ticket buyer the number (unknown to the ticket seller) in accompaniment to the secure second transformation. Thus, there is no division of steps in generation of the digital ticket in Mengin. Instead, all of the security measures for a digital ticket in Mengin between the ticket buyer and the ticket seller appear to benefit only one party, the ticket seller.

Accordingly, Mengin fails to teach or suggest several of the features defined in independent claim 51. Applicants thus respectfully request reconsideration and withdrawal of the rejection of claim 51 and dependent claims 52-55.

Claims 1, 8, 24, 30, 32-37, and 48-50 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Rosen, and with respect to claim 48 in view of Mengin et al. Claim 24 has been amended to incorporate features of allowable claim 25 (which has now been cancelled). Applicants respectfully traverse the rejection of the remaining claims for at least the following reasons.

Regarding the rejection of claim 1, the pending Office Action states, “Please see the last office action as examiner maintain the previous Examiner’s office action in that regard.” However, in the last Office Action, mailed May 27, 2005, claim 1 was stated to be allowable if rewritten to overcome the previous 35 U.S.C. § 112, second paragraph, rejection (now withdrawn). The new Office Action does not state why the previous statement re allowance of claim 1 was removed, nor does it state why Applicants’ previous remarks regarding the patentability of claim 1, which were previously accepted, are now apparently dismissed. Thus, Applicants have not been provided a fair opportunity to respond to the

rejection of claim 1, as they are not sure what issues exist as to patentability. More particularly, Applicants have received no response to the argument, submitted in Response B, filed March 24, 2005, that Rosen fails to teach or suggest a digital signature of digital data D_3 in respect of first or second digital data D_1 or D_2 as defined in claim 1.

Accordingly, Applicants herein incorporate by reference the remarks in Response B, filed March 24, 2005 re claim 1, which were previously accepted. Further, for at least this reason, Applicants respectfully request, if the rejection is maintained, that the finality of the pending Office Action be withdrawn and a new, non-final Office Action be issued.

Regarding claims 8, 30, 32-37, and 48-50, the Office Action cites col. 11, lines 14-67 and col. 12, lines 1-15 of Rosen as teaching a **Sign (s, I || hash (R)) || R** digital ticket. However, the process described in the cited section is for certification of trusted servers or trusted agents, not for generation of digital tickets. In Rosen, digital tickets are created separately. The Office Action does not appear to submit a reason that a process for certification would teach or suggest a process for generating a digital ticket, particularly when Rosen itself teaches a separate digital ticket generation process.

Furthermore, the cited section of Rosen fails to teach or suggest the **Sign (s, I || hash (R)) || R** digital ticket defined in claims 8, 30, 32, 33, and 48. As stated above, the digital ticket and the process for creation thereof in embodiments of the present invention allow two parties, such as a ticket buyer and a ticket seller, to together produce a digital ticket

that provides protection for both parties against possible fraud by the other party, without requiring outside certification.

However, even assuming only for the sake of argument that the process for generating a certificate described in Rosen teaches or suggests a process for generating digital tickets, this process is performed entirely by one party. For example, the formula for certifying a trusted server from a primary trusted server in Rosen is set forth below:

$$\text{Cert}(\text{TS}) = E_{PTS}[\text{TS}(\text{id}) \parallel \text{TS}(\text{PK}) \parallel \text{expire date} \parallel \sigma_{PTS}(X) \parallel \text{PTS}(\text{id})]$$

X

$$\text{Cert}(\text{TA}) = E_{TS}[\text{TA}(\text{id}) \parallel \text{TA}(\text{PK}) \parallel \text{expire date} \parallel \sigma_{TS}(Y) \parallel \text{Cert}(\text{TS})]$$

Y

Where

PTS = Primary Trusted Server

TS = Trusted Server

TA = Trusted Agent

\parallel = Concatenate

id = identification number

PK = Public Key

σ = digital signature

Cert = Certificate

E = Algorithm with private key used for encrypting
and for creating digital signature

The certificate validation protocols are:

1) Validate Cert (TS)

a) $D_{PTS}(E_{PTS}(X \parallel \sigma_{PTS}(X))) = X \parallel \sigma_{PTS}(X)$

b) Check if date is valid

c) Check if $D_{PTS}(\sigma_{PTS}(X)) = h(X)$

2) Validate Cert (TA)

a) Validate Cert (TS)

b) $D_{TS}(E_{TS}(Y \parallel \sigma_{TS}(Y))) = Y \parallel \sigma_{TS}(Y)$

c) Check if date is valid

d) Check if $D_{TS}(\sigma_{TS}(Y)) = h(Y)$

Where

h=hash function used in creating and checking digital
signature (i.e., one-way function)

D= Algorithm with public key used for decryption and
for checking digital signature

$\sigma = E \circ h$

Note E and D may also be used for decrypting and
encrypting, respectively, when applied in other
applications.

As provided in Rosen, to certify a trusted agent, the trusted server assigns a unique ID, which is $T(id)$. The trusted agent passes a public key ($TA(PK)$) to the trusted server. The trusted server, and only the trusted server, then: (1) concatenates $TA(id)$, ($TA(PK)$) and expire data to provide a number Y (that is, the number is generated by the trusted server, and there is no number used in generation of the certificate that is private to the trusted agent); (2) hashes the number to provide $h(Y)$; (3) encrypts the hashed number to provide $\sigma_{TS}(Y)$; (4) concatenates $\sigma_{TS}(Y)$ with Y ; (5) encrypts (E_{TS}) the concatenation of $\sigma_{TS}(Y)$ and Y ; and (6) concatenates this encryption with the trusted server's certificate $Cert(TS)$.

Therefore, each part of the trusted agent certificate is Rosen is generated only by one party – the trusted server. Certification of a trusted server by a primary trusted server operates substantially the same way, except the primary trusted server generates the entire digital certificate.

Additionally, Rosen fails to teach or suggest that a party other than the party providing the digital signature appends the original number to form a digital ticket. Instead, in Rosen, a single party produces a number (X or Y), hashes the number, encrypts the hashed number, concatenates X or Y , encrypts this concatenation, and appends either a primary trusted server ID or a trusted server certificate ($Cert(TS)$).

Thus, in Rosen the generation of a certification is performed by a single party for the security of that single party vis-à-vis the party receiving the certification. This is not the same as the multi-party digital ticket generation method and system defined in claims 8,

30, 32-37, 48, 49, and 50. Further, as to claim 48, Mengin fails to remedy the deficiencies of Rosen, as it discloses a process for generating a digital ticket in which a number, hashed number, and encrypted hashed number are all generated from a single party, as explained above.

Additionally, neither certification structure shown above in Rosen appears to teach or suggest the additional information I that is signed before appending the original number R in digital ticket **Sign (s, I || hash (R)) || R**. As shown, formula $\sigma_{TS}(Y)$ or $\sigma_{PTS}(X)$ apparently includes a digital signature of a hashed X or Y, but not of additional information. Further, original number X or Y is only appended to $\sigma_{TS}(Y)$ or $\sigma_{PTS}(X)$ before encryption E_{TS} or E_{PTS} . Any additional information is appended after this encryption, not within the encryption.

For similar reasons, Rosen fails to teach or suggest all of the features in claims 34-37, 49, and 50. For example, regarding claims 34-37, Rosen fails to teach or suggest second-type data generated first by a ticket buyer as a non-invertible function of a random number called a “first-time-made non-invertible function,” second by the ticket seller as a digital signature of the first-time-made non-invertible function, and third by the buyer of the ticket to attach the self-same random number. Additionally, Rosen fails to teach that a random number is used, and in fact teaches away from this, as the numbers X and Y consist of identification numbers, a public key, and expiration data. Regarding claims 49-50, Rosen fails to teach or suggest at least a ticket buyer computer sending at a first time a one-way transformation of a private number to a seller computer, a ticket seller computer receiving the

one-way transformation and signing the one-way transformation and additional information, the ticket seller computer sending the signed first transformation and additional information to the ticket buyer computer as signed information, and the ticket buyer computer storing the received signed information plus the private number.

Accordingly, Applicants respectfully submit that claims 1, 8, 30, 32-37, and 48-50 are allowable over the references of record, including Rosen and Mengin. Applicants thus respectfully request reconsideration and withdrawal of the rejection.

For at least the foregoing reasons, Applicants believe that this case is in condition for allowance, which is respectfully requested. The Examiner should call Applicants' attorney if an interview would expedite prosecution.


Respectfully submitted,
GREER, BURNS & CRAIN, LTD.

Customer No. 24978

January 17, 2006

300 South Wacker Drive
Suite 2500
Chicago, Illinois 60606
Telephone: (312) 360-0080
Facsimile: (312) 360-9315

P:\DOCS\0321\67683\9S4440.DOC

By: 
Arik B. Ranson
Registration No. 43,874